Consiglio Nazionale delle Ricerche

Biometrics authentication with smartcard

L. Bechelli, S. Bistarelli, A. Vaccarelli

IIT TR-08/2002

Technical report

Maggio 2002

Istituto di Informatica e Telematica

Biometrics authentication with smartcard*

IIT TR-08/2002

Luca Bechelli[1], Stefano Bistarelli[1], and Anna Vaccarelli[1]

Istituto di Informatica e Telematica (IIT), CNR Pisa,
Area della Ricerca di Pisa, Via G. Moruzzi 1, I-56124 Pisa, Italy,
{L.Bechelli,S.Bistarelli,A.Vaccarelli}@iit.cnr.it,
http://www.iat.cnr.it/attivita/progetti/parametri_biomedici.html

Abstract. The purpose of this paper is to highlight and solve issues concerning the biometric information for authentication and their use with smartcards.

Keywords: biometric information, smartcard.

1 Fingerprint storage and matching systems through smartcard

The system we are going to describe may use different technologies to match fingerprints acquired by a biometric scanner with stored templates. In particular, it is possible to identify three different possibilities for the use of microcircuit or microprocessor cards within systems which support biometric identification devices:

Template on Card: This class groups those applications and systems where the biometric template is stored on a hardware security module (smartcard or USB token). In this case the template has to be retrieved and transmitted to a different system to compare the fingerprints acquired by special scanners; "memory-cards" with no operating systems and onboard applications are generally used for this purpose.

Match on Card: This class groups those applications and systems where the comparison between the biometric template and the fingerprint acquired through a special scanner occurs inside a hardware security module. This is typically achieved through the use of a smartcard microprocessor provided with an operating system and suitable applications and the biometric template is *safely* stored on the card itself.

* phase 1 of the project "ACCORDO DI COLLABORAZIONE SCIENTIFICA TRA ISTITUTO PER LE APPLICAZIONI TELEMATICHE DEL CNR e CENTRO BIOMETRIKA S.R.L"

System on Card: This is an evolution of the two technologies above and is certainly the best solution in terms of security because it includes the use of hardware security modules hosting biometric scanners where the acquisition, processing, template selection and match operations occur within a totally secure system. This type of technology is realized through the use of smartcards with piezoelectric fingerprint readers or USB tokens equipped with special fingerprint scanners. The use of USB token-based systems is preferred since they do not need a special smartcard reader but are directly connected to the host processing system.

1.1 Description of the system

In the following we will illustrate some systems that can provide safe access to protected data inside a hardware token: the case at issue can be compared to the safe access problem concerning private asymmetrical keys stored on a cryptographic smartcard. In the proposed system, once the fingerprint (the authentication credential) has been acquired, the match occurs within an objective system such as a smartcard which contains previously acquired (during card enrolment) safe templates. This system can be summarised as shown in Figure 1 where:

1. The fingerprint reader detects the live fingerprint,
2. The user's machine host system, which receives the acquired fingerprint, processes and sends it to the smartcard,
3. The smartcard, after receiving the fingerprint, compares it to the template and returns an authenticated session answer to the calling user application.

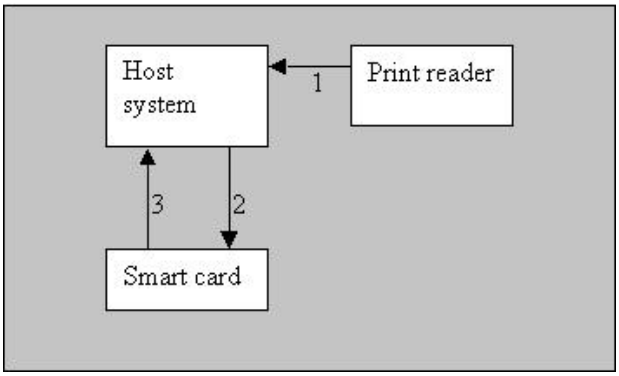

Fig. 1. Smartcard-Scanner system Description.

However, the system outlined above is susceptible to many potential safety attacks and therefore each one of the information transfers, as per 1,2,3, will have

to occur through the use of special communication protocols. The reliability and safety of the host system, fingerprint reader and smart card have to be guaranteed and furthermore a solution that increases or at least maintains the security level obtained with a Personal Identification Number (PIN) will have to be specified. The safety has to be maintained both if the card is used according to traditional mechanisms and applications and if it is used in a context in which biometric fingerprints are used to strengthen and accelerate authentication procedures. One must bear in mind that smartcards owe their popularity and widespread use in many application environments to there high safety level, easy use and portability from one system to another. In theory, an equivalent scheme, in terms of safety, to the use of a PIN could result inefficient or ineffective, whereas in practice the correct use of a PIN poses some problems:

- PIN's are typically composed of only numerical digits;
- PIN's can be difficult to remember and are often forgotten;
- Generally people choose simple PIN's and this reduces remarkably the card's safety level;
- A prolonged use of the same PIN over time can, under some circumstances, expose it to brute attacks.

Generally, these issues are ideally solved by biometric identification.

The specifications required to guarantee the safety level of the system communication and hardware are outlined below.

1.2 Subjects involved in the system

Before specifying in detail the logon smartcard system, a clearer illustration of the features of subjects involved in the authentication process is undertaken:

scanner system intends the biometric fingerprint reader built in the safe communication system that we are going to examine. In real setups, this system could be implemented via one single device connected to a PC, or two separated processing systems physically connected through a 'trusted' communication medium which is not susceptible to logic or physical attacks that try to alter or replace the Protocol Data Units (PDUs) as they transit.

token intends a hardware security module that complies with ISO 7816 I, II, III and IV specifications and that is provided with functions implementing symmetric and asymmetric cryptographic algorithms. In a real setting, this system could be implemented via a smartcard, a USB token or a board with a cryptographic processor. A simpler prototype could consist in a hardware security module connected to a processing system through a 'trusted' communication medium which is not susceptible to any logic or physical attack that try to alter or replace the PDUs as they transit. For production environments, the token should only be considered as a totally isolated system.

2 User-smartcard authentication protocol based on biometric identification systems

Accessing a smartcard through biometric identification systems must include an authentication measure to guarantee that the protection level is at least equivalent to that of a traditional PIN.

For this reason, the fingerprint detection system (scanner system) should be recognizable as *trusted* by the token system in order to guarantee that the transmitted biometric fingerprint has been acquired *live*.

2.1 Attacks and vulnerability of the biometric logon system on smartcard

The scheme presented is not secure because biometric information used to provide access is:

- the same throughout the user's life: this makes it impossible to change the access credential to a system more than 10 times (once for each finger!).
- public, i.e. even though it is difficult to acquire and typically regarded as a private detail in reality it is issued hundreds of times per day in uncontrolled (and therefore hostile by definition) settings.
- different at each acquisition: this is why it cannot be used to generate a normalized detail that is always the same and therefore cannot be applied to generate an unalterable password. Moreover, being a public detail, it cannot be used to generate a secret key or PIN.

The major risk posed by the use of biometric systems in an authentication process is that a malicious subject may intefere with the communication and intercept the biometric template and use it later to obtain access. Likewise, an attack may be committed by generating a template from a fingerprint obtained from some surface. Both attempts are based on the exclusion of the scanner and on the submission of the template through a different channel. Secondary attacks brought against the smartcard are:

- DoS (Denial of Service): since most logon smartcard procedures provide for a maximum number of attempts, incorrect or false details may be sent to the card to stop access. This attack is even more detrimental if the card has no releasing procedure (such as PKCS#11 smartcards in general)
- Attacks against the biometrical matching procedure by exploiting any vulnerability of the Match On Card software (ex: buffer overflow) or a bad balancing between false positives and false negatives.
- Attacks against the smartcard, i.e. attacks trying to alter details, which the card uses to carry out the Match on Card algorithm, such as the biometric template in order to replace it with that of the attacker (identity replacement) or system variables which are altered forever (DoS attack)

2.2 Scanner system - token communication protocol

The scanner-token communication protocol must ensure:

- Authentication of the scanner system to the token
- Authenticity of the biometric information transmitted by the scanner system
- Integrity of the exchanged information
- Non-repeatability of the process, to avoid attacks based on the repetition of PDUs exchanged by different subjects.

Compliance with these requirements will ensure that:

- the fingerprint comes from an authorized scanner
- the fingerprint has been acquired live (livescan)
- the biometric information has not been altered during communication

The steps included in the communication protocol are summarized in the diagram below:

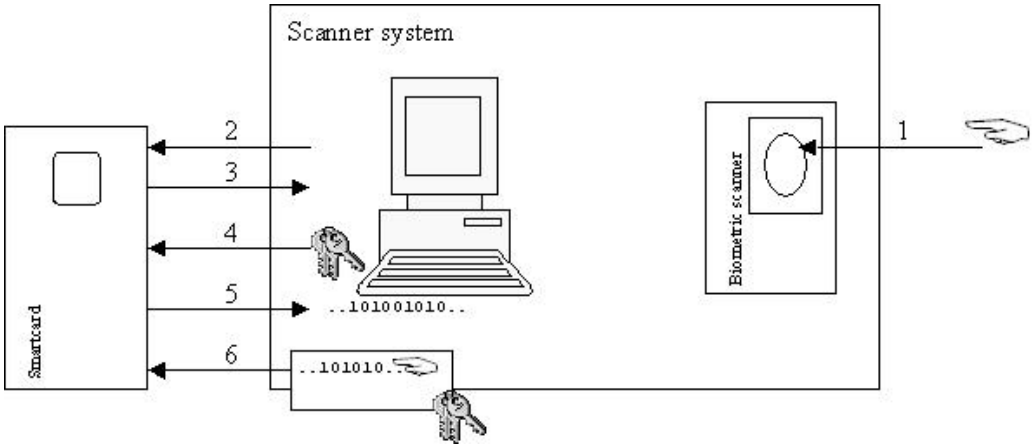

Fig. 2. Communication protocol between smartcard and scanner system.

1. The user places his/her fingerprint on the scanner
2. The scanner requests the token to be allowed to send the fingerprint
3. The token requests the scanner to supply its authentication credentials
4. The scanner supplies its credentials
5. The token checks the scanner's authentication credentials and, if sufficient, replies with a challenge, i.e. a randomly generated number
6. The scanner acquires the fingerprint and processes it along with the challenge using, if required, cryptographic functions or the same authentication credentials. Finally, the processed fingerprint is sent to the token

7. The token checks that the challenge matches the one sent and then submits the fingerprint to the functions required to check for authenticity and integrity. Upon verification, the token matches the live fingerprint and template contained in a protected area
8. If the match is positive, the token returns a handler of the communication session to the user.

When checking the protocol for safety, the following factors are affected:

1. Safety level of the scanner system: this parameter analyzes the risk factor associated to the scanner system, i.e. the likelihood that logical or physical attacks may occur or the fact that transiting information or authentication credentials may be intercepted/altered.
2. Safety level associated to the random generator of the token system: this factor affects the quality of the challenges and any one-time cryptographic key generated by the token system. If the random generator has an excessively low repeat frequency, an attacker might try to track down the cryptographic keys used or prepare messages using someone else's credentials and the challenges that the attacker expects the token system to generate.
3. Safety level of the authentication function of the scanner system: this factor affects the risk that an attacker may interfere actively between two systems and submit false biometric information for unauthorized access to the smartcard. In traditional systems, the protection level of the smartcard data is protected by the PIN and it can be reasonably assumed that the safety level of the card, in this implementation, is equivalent to the safety extent obtained by the connecting authentication function between the two devices. In addition, the quality of scanner authentication credentials somehow guarantees the fingerprint and is also the basis for the protocol applied.
4. Correct balancing between false positives and false negatives and accuracy level of the biometric match between the "live" fingerprint and the template contained on the smartcard
5. Protection level of the fingerprint template inside the smartcard: any unauthorized access to the biometric fingerprint attempting to alter or replace the template would expose the entire system to attacks concerning availability and confidentiality of the data contained on the smartcard.

An in-deep analysis will not consider factors 1, 2, 4, and 5[1] since many do not essentially depend on the protocol we are going to analyze but are inherent in the devices themselves. In order to more accurately determine the protection level of the overall logon smartcard system, the entire evaluation will be based on the authentication system and credentials of the scanner system.

2.3 Scanner system authentication

The safety and complexity level of the scanner system authentication procedure can be adjusted to the required safety level. In particular, possible variants are

[1] Due to be conducted at a later stage of the Scientific Co-operation Agreement, Technical Annex, item 2.

considered based on the of the type of authentication credentials used, starting from the highest safety level:

- X.509 digital certificates
- password dynamically entered by the user
- shared password

X.509 digital certificates. In this scheme, the scanner system is associated to a digital certificate with a pair of asymmetrical keys, for instance RSA. Using digital certificates, the scanner-token communication protocol can be revised as follows:

1. The user places his/her fingerprint on the scanner
2.-4. The scanner requests the token to be allowed to send the fingerprint and submits the request by digitally signing it and enclosing its certificate
5. The token checks the signature for authenticity and integrity, then generates a challenge (i.e. a randomly generated number) and codes it using the scanner's public key
6. The scanner acquires the fingerprint and codes it with the challenge received from the token after decoding it.
7. Using the challenge, the token decodes the received data and if the operation is successful, it matches the live fingerprint with the template contained in a protected area
8. If the match is positive, the token returns a session communication handler to the user.

To support the protocol above, the scanner system must have a set of APIs or a hardware device available to safely store the private key and must be able to digitally sign the information sent from the scanner. The token, in its turn, must have a copy of the certificate of the CA that issued the certificate associated to the scanner. The safety level of the described system depends on:

- the safety level of the protection system of the private key associated to the scanner
- the safety level of the certificate enrolment procedure as well as the way the CA certificate is stored in the smartcard

It is now clear as to why a cryptographic system having the same safety characteristics as a Hardware Security Module should be included in the scanner system. In addition, the CA certificate must be stored on the token as an unchangeable file in order that it may not be deleted, replaced or altered by anyone else without the required authorizations.

The CA that issues the certificates associated to the scanner may be managed by the device supplier or be a CA at the service of the client company (who uses token-scanner devices) if a higher safety level is required. The described system offers the following advantages:

- The scanner-token messages cannot be repudiated

– The messages are checked for integrity
– Any scanner system can be used, provided it is certified by the CA and the token considers it as 'trusted'
– A highly automated scanner-token communication protocol is achieved

Enrolment procedure for scanner system certificates. The scanner system certificate can be issued by the CA using a standard procedure, as described in the SCEP protocol [1]. The advantage of using this protocol lies in the fact that the entire procedure can take place without involving the end user. Of course, the use of any automatic system, however standard it may be, needs the scanner system to be provided with suitable implementation software.

Password dynamically entered by the user. This scheme replaces the use of digital certificates with a simpler mechanism where no credentials have to be stored. The scanner-token communication uses a shared symmetrical key, which is supplied by the user upon starting the protocol:

1. The user places his/her fingerprint on the scanner
2. The scanner requests the token to be allowed to send the fingerprint
3. The token requests the scanner to supply its authentication credentials
4. The scanner requests the user to enter the password that will then be sent to the token
5. The token checks the scanner's authentication credentials and if verified replies with a challenge (i.e. a randomly generated number) coding it with the user password.
6. The scanner acquires the fingerprint and codes it using the (decrypted) challenge as the key. Finally, the coded fingerprint is sent to the token
7. Using the challenge, the token decodes the received fingerprint. If verified, it matches the live fingerprint with the template contained in a protected area.
8. If the match is positive, the token returns to the user a handle of the communication session.

When starting the next access request, the scanner will not request the user to re-enter the password, nor need it store a copy in cache memory but can automatically send the previously generated challenge to obtain a subsequent new challenge. The process can be repeated several times, provided that the token re-initialized once it is taken out of the reader requiring user password for further use.

For simplicity, the user password, as per item 4 above, can be assumed to be equivalent to the traditional token access PIN. Nevertheless, the described system is interesting and useful for two reasons:

– If an application requires authentication towards the smartcard several times within one working session, the user does not need to enter the PIN every time but only place his/her finger on the scanner. This applies, for example, to legally valid digital signatures as laid down by the DPCM 8/2/99.

– The described system strengthens the safety level of the logon smartcard procedure, since it necessarily requires the card-holder's presence.

In addition, the described procedure is applicable to all of the scanner systems that support the protocol since the credentials are not encoded within the scanner system.

Shared password. This scheme consists in the sharing of a symmetrical key by the scanner and token. The key may differ for each scanner or may be encoded within the fingerprint acquisition device. The communication protocol thus becomes the following:

1. The user places his/her fingerprint on the scanner
2. The scanner requests the token to be allowed to send the fingerprint information
3. The token replies with a challenge, i.e. a randomly generated number

4.-6. The scanner acquires the fingerprint and codes it along with the challenge using the shared password as a key. Finally, the processed fingerprint information is sent to the token

7. The token decodes the received message, separates the challenge from the fingerprint information and checks for match. If this results in success, it matches the live fingerprint with the template contained in a protected area
8. Upon positive outcome, the token returns to the user a handle of the communication session.

The safety level of the described system is equivalent to the protection level of the password shared between scanner and token. Of course, if choosing to use one single key for all scanner devices, the safety level will further decrease, while the smartcard will be usable with any scanner supplied by the same manufacturer. Alternatively, if there is only one password per scanner (that could be personally determined by the user when installing the device), biometrical identification cannot be used unless with a well-defined user platform. with this latter method, the password might have to be changed from time to time. Finally, in the case where the user uses several tokens, the user will have to use the same password for all tokens. In the described scheme, the shared password should not be the traditional PIN of the smartcard in oder not to decrease the safety level of the token outside the environment in which the traditional authentication function is used. Finally, the scanner system will have to be equipped with suitable password protection mechanisms for the instrument to withstand logical or physical attacks.

3 Prototype development

Developing a prototype requires adequate know-how and resource investments in order to achieve a gradual analysis and implementation process with the intent to identify any potential use of the acquired notions. It is not excluded that

functionality and technology might lie beyond the objectiveness of the system. For this reason, the following assumptions will be made:

step 1: during the protocol implementation through *template on card* technology: the host to which the reader and the smartcard is connected is identified as the *token system*. Fingerprint matching and processing operations will be carried out on the host, while the template and any information required for the authentication process will be hosted by the smartcard

step 2: validity of specification item 3 in protocol, as provided by the Scientific Co-operation Agreement, Technical Annex. Feasibility of specifications through "match on card" technology is due to be assessed at a later stage (*possibly at times and through methods to be agreed in consultation with Centro Biometrika*).

step 3: protocol implementation meeting specifications as per **step 2**. *Times and methods to be agreed in consultation with Centro Biometrika.*

The purpose of the preliminary **step 1** is to acquire the knowledge required for the development of an authentication system prototype on a local system based on biometric identification media and smartcard, as described below.

3.1 Local-system logon procedure through biometric identification media and smartcard with "Template on Card" technology

Using local-system biometric media for identification implies that the biometric detection system can be reasonably regarded as "trusted" by the host itself.

Whenever we are sure 1) that the host is physically connected to a 'trusted' scanner and 2) that the biometric information has been received only through physical connection to this device, we can assumedly speak of *biometric authentication*.

Of course, the conditions above are actually very strict constraints which practically are not always easy to apply and control but are still indispensable conditions to be sure that the fingerprint received by the host has been acquired through **livescan**. If requirements as per items 1) and 2) should be difficult to obtain or check, once again a similar protocol to that described in Section 2.2 will have to be applied to guarantee the actual fingerprint *livescan*. In many instances, however, this scheme is not applicable due to technological or even legal constraints. Leaving out an accurate list of case-studies which would be in any case incomplete or not deep enough, we look at two emblematic and extremely frequent instances:

Host authentication with domain server: This is the case of host access in a network with only one authenticator/domain server where users are not locally registered but are defined instead on one single system which possesses the authentication credentials and authorization profiles. Under these circumstances, access authorization cannot be issued to a local system by sending the biometrical fingerprint to the central server, since this could result in the problems that have been described above for safe smartcard access.

Biometric authentication by maintaining user privacy This is the case when, due to the constraints enforced by confidentiality regulations, the users' biometric fingerprints cannot be stored on a host.

Both problems can be solved in the same way and involves increasing the safety level through the addition of an *authentication factor*: **possession**. In both cases, the users are assumed to possess a smartcard, not necessarily one with a microprocessor, but a simple *memory card* on which a biometric template is stored. Under these conditions, the matching between the acquired fingerprint and the template is carried out on the host system which takes the template from the card after having somehow recognized it: if card recognition and fingerprint comparison are successful, the user is granted access to the system. The scanner-host-smartcard communication protocol can be summarized as follows:

1. The user places his/her fingerprint on the scanner
2. The authentication application on the host receives the fingerprint and requests the smartcard to authenticate itself to the system
3. The smartcard provides its authentication credential and fingerprint template to the application on the host
4. The application checks the card's authentication credentials and if correct matches the received template with the fingerprint acquired by the scanner
5. If the match is correct, the application authorizes user's access

In this case, the user supplies the authentication system with two different pieces of information:

- What the user is (biometric information)
- Something the user possesses (smartcard)

with the advantage that the biometric template does not have to be stored on the host or server. Digital signature-based mechanisms can guarantee the template's integrity and authenticity within the smartcard, but the safety level of the entire scheme certainly depends once again on the two assumptions made above:

- The scanner is physically connected to the host
- Biometric information is safely received from the scanner

Host authentication with domain server. Here, the authentication server cannot use biometric information to authenticate users unless it trusts the user host system. In this scenario, the logon application generally receives from the host either biometric information digitally signed with the host's key (similar to the smartcard authentication protocols previously described), or obtains a username and password couplet supplied by the host if the host recognizes the user through a biometric identification process. The use of VPNs on local networks and environmental safety mechanisms may contribute to the building of absolutely 'trusted' network logical areas that fulfill the requirements above. In view of increasing the safety level of the described scheme, the smartcard could

be provided with *on board* software for extraction or assistance in the building of the authentication credentials to be sent to the domain server: for instance, when requested by the application on the host system, it could digitally sign an access request to be addressed to the server. It could also establish a safe channel with the server itself using on board cryptographic keys for the transit of a ¡userid,password¿ pair stored in the card's file system.

Acknowledgements. We are indebted to Claud Anticoli for a careful reading of the paper that help us to cut away many typing errors.

References

[1] : Cisco system's simple certificate enrollment protocol. White paper, (Cisco)
[2] : Internet x.509 public key infrastructure qualified certificates profile. (RFC 3039)
[3] : Biometric device protection profile. Draft 0.82, (UK Government Biometrics Working Group)
[4] : R22 user authentication techniques using public key certificates. part 2: Authentication information including biometrics. Technical report, (U.S. National Security Agency, Central Security Service)
[5] : R22 guidelines for placing biometrics in smartcards. Technical Report Version 1.0, (U.S. National Security Agency, Central Security Service)